Published and Copyright (c) 1999 - 2012
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1429 07/27/12

~ America's Failing Grade ~ People Are Talking! ~ 'World of Warcraft'!
~ IOC: Watch Your Tweets! ~ Twitter Threat Appeal ~ Mac Malware Alert!
~ OS X Mountain Lion News ~ Who Invented Internet? ~ The Future of Games!

~ Facebook Stock Tanking! ~ ~ AOL Dial-up Hell!

-* Hackers Get Yahoo Passwords! *-
-* Cyber Commander's Makes Accusations *-
-* U.S. Spy Agency Chief To Meet at 'Defcon'! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

I apologize for the tardiness of this week's issue. A lot of personal issues, culminating with some legal proceedings dealing with my late father's estate, have not enabled me much time to work on this week's issue. Fact is, there are many more important things going on in my life these days for me to really be overly concerned about A-ONE and other pasttimes. I hope that you'll indulge me during these times.

Until next time...

=~=~=~=

->In This Week's Gaming Section - 'World of Warcraft' To Receive Expansion!
"""""""""""""""""""""""""""""""" The Future of Games, Wearable Computers

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

'World of Warcraft' To Receive Expansion in September

World of Warcraft's fourth expansion, the panda bear feature Mists of Pandaria, is to be made available from September 25.

Players allied with either of the game's factions, the Alliance or the Horde, will be ushered towards the lost continent Pandaria, where a new type of playable character awaits, the bear-like Pandaren.

The expansion is intentionally aimed at World of Warcraft old-timers, casual players and newcomers alike, with the panda motif expected to go

down particularly well with World of Warcraft’s Chinese user base.

In addition, Mists of Pandaria’s release is well-timed to woo back ex-WoW players who have been checking out other titles in the Massively Multiplayer Online game genre, in particular Guild Wars 2, which launches a month prior, on August 28.

Official website: battle.net/wow/game/mists-of-pandaria/

Valve s Gabe Newell on The Future of Games, Wearable Computers, More

Gabe Newell, the co-founder and managing director of Valve, the videogame development and online distribution company, made a rare appearance last night at Casual Connect, an annual videogame conference in Seattle.

Newell, who spent 13 years at Microsoft working on Windows, is not well-known outside of the videogame industry, but the company he has built in Bellevue, Wash., cannot be overlooked.

Valve is not only a game developer, producing megahits like Portal 2, it owns and operates Steam, which is the largest consumer-focused digital games distribution platform in the industry. By some measures, it may be valued at $3 billion.

Last night, at a dinner sponsored by Covert & Co., Google Ventures and Perkins Coie, Newell unveiled some of his most quirky and secretive projects in an interview onstage with Ed Fries, former VP of game publishing at Microsoft.

Newell, who has a desk on wheels so he can quickly roll over to his favorite projects within the company, struggled at times to put into words how he sees the industry shaking out as companies like Microsoft and Apple move toward closed ecosystems. At one point, he even lamented that his presentation skills aren t up to speed because Valve isn t a public company.

Here are excerpts from the conversation that took place in a packed and noisy room with an under-powered speaker system:

On the future of videogame distribution

Everything we are doing is not going to matter in the future. We think about knitting together a platform for productivity, which sounds kind of weird, but what we are interested in is bringing together a platform where people s actions create value for other people when they play. That s the reason we hired an economist.

We think the future is very different [from] successes we ve had in the past. When you are playing a game, you are trying to think about creating value for other players, so the line between content player and creator is really fuzzy. We have a kid in Kansas making $150,000 a year making [virtual] hats. But that s just a starting point.

That causes us to have conversations with Adobe, and we say the next version of Photoshop should look like a free-to-play game, and they say, We have absolutely no idea what you are talking about, but it sounds really bad. And, then we say, No, no, no. We think you are going to

increase the value being created to your users, and you will create a market for their goods on a worldwide basis. But that takes a longer sell.

 This isn t about videogames; it s about thinking about goods and services in a digital world.

On closed versus open platforms

 In order for innovation to happen, a bunch of things that aren t happening on closed platforms need to occur. Valve wouldn t exist today without the PC, or Epic, or Zynga, or Google. They all wouldn t have existed without the openness of the platform. There s a strong tempation to close the platform, because they look at what they can accomplish when they limit the competitors access to the platform, and they say That s really exciting.

 We are looking at the platform and saying, We ve been a free rider, and we ve been able to benefit from everything that went into PCs and the Internet, and we have to continue to figure out how there will be open platforms.

On Valve s interest in Linux

 The big problem that is holding back Linux is games. People don t realize how critical games are in driving consumer purchasing behavior.

 We want to make it as easy as possible for the 2,500 games on Steam to run on Linux as well. It s a hedging strategy. I think Windows 8 is a catastrophe for everyone in the PC space. I think we ll lose some of the top-tier PC/OEMs, who will exit the market. I think margins will be destroyed for a bunch of people. If that s true, then it will be good to have alternatives to hedge against that eventuality.

On the evolution of touch

 We think touch is short-term. The mouse and keyboard were stable for 25 years, but I think touch will be stable for 10 years. Post-touch will be stable for a really long time, longer than 25 years.

 Post touch, depending on how sci-fi you want to get, is a couple of different technologies combined together. The two problems are input and output. I haven t had to do any presentations on this because I m not a public company, so I don t have any pretty slides.

 There s some crazy speculative stuff. This is super nerdy, and you can tease us years from now, but as it turns out, your tongue is one of the best mechanical systems to your brain, but it s disconcerting to have the person sitting next you go blah, blah, blah, blah.

 I don t think tongue input will happen, but I do think we will have bands on our wrists, and you ll be doing something with your hands, which are really expressive.

On wearable computers

 I can go into the room and put on the $70,000 system we ve built, and I look around the room with the software they ve written, and they can overlay information on objects regardless of what my head or eyes are doing. Your eyes are troublesome buggers.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

America’s Failing Grade on Cyber Attack Readiness

The man in charge of America’s cyber operations said that on a scale of one to 10, the nation’s preparedness to deal with a major cyber attack on critical infrastructure sits at a dismal three.

"Somebody who finds vulnerability in our infrastructure could cause tremendous problems," Army Gen. Keith Alexander, Director of the National Security Agency and chief of U.S. Cyber Command, told audience members at the Aspen Institute’s annual security forum late Thursday, according to multiple reports. Alexander said that since 2009, attempted cyber attacks on the nation’s infrastructure systems have risen seventeen-fold.

"I’m worried most about power. I’m worried about water. I think those are the ones that need the most help," he said.

Top current and former U.S. security officials have for years been decrying vulnerabilities in the computer networks of critical infrastructure industries from water treatment centers to electric power plants - largely facilities owned and operated by private entities. In his remarks, Alexander reportedly pushed for greater role of government, specifically the Department of Homeland Security, in regulating security measures across industries.

Two years ago, computer experts discovered Stuxnet, a cyber weapon of unprecedented power and complexity that was apparently designed to damage an Iranian nuclear facility. The worm had demonstrated what computer experts had long though possible but had never actually seen: computer code that was no longer confined to disrupting computer systems internally but could reach out and physically alter how a facility works, or potentially destroy it.

Before the worm was alleged to have been a creation of a joint U.S.-Israeli cyber operation, other U.S. officials quickly realized that such a powerful cyber tool may be turned on the homeland. In a Senate Homeland Security committee hearing in November 2010, committee chairman Joe Lieberman (D.-Connecticut) warned the worm could be used as a "blueprint" for other "malicious hackers."

Richard Clarke, former White House counterterrorism advisor, cyber security expert and ABC News consultant, said in January that since Stuxnet was a "plug-and-play" worm, other hackers or foreign governments could take it, modify it and turn it against the U.S.

"You can take out certain components and put in others and you have a very powerful weapon that could be used against the electric power grid or any other system that has computers telling machines what to do," he said.

"The best cyber weapon in the world has been spread around for other people to have copies of I think it’s very likely that somebody could do this."

Months later, the Department of Homeland Security revealed that the original Stuxnet worm did manage to infiltrate a computer system in the U.S., but since it was only tailored to hit the Iranian nuclear facility, it didn’t do any known damage to the American facility.

Sean McGurk, a former DHS official who is now senior policy officer at the Industrial Controls Systems Information Sharing and Analysis Center, told a radio show in early June that he had already seen hackers modifying Stuxnet for their own uses. He also noted that as one of the most computer-reliant nations on the planet, the U.S. is also one of the most vulnerable.

"Because everything from elevators to prison doors are controlled by computers in our country, these systems lend themselves to manipulation and potentially to destruction," he said.

Since Stuxnet’s discovery, cyber experts have found two other highly-sophisticated cyber weapons: Duqu, a cyber program built in the style of Stuxnet but for espionage rather than offensive operations, and Flame, the largest espionage program in history designed to capture any keystroke, image and conversation even near the infected system. Based on stunning similarities in the code of all three programs, researchers said they believe they were all created by either the same team, or at least teams of computer experts with access to each other’s original work.

Cyber Commander Accuses Countries of Targeting Infrastructure

Unspecified nations played a role in a 17-fold jump in cyber attacks on U.S. infrastructure since 2009, but this does not appear to reflect payback for a reported U.S. role in malicious code known as Stuxnet, the head of the Pentagon’s National Security Agency said on Thursday.

"I don’t see the correlation there at all," Army General Keith Alexander told a security forum in Aspen, Colorado. "I don’t see anything that goes to Stuxnet or anything like that."

Stuxnet was the first discovered malware designed to subvert industrial systems. Credited with setting back Iran’s disputed nuclear program, it has been reported by The New York Times to have been part of a U.S. and Israeli intelligence operation started under President George W. Bush and expanded under President Barack Obama.

The Office of the National Counterintelligence Executive, a U.S. intelligence arm, said in a report to Congress in October that China and Russia were in the forefront of keyboard-launched theft of U.S. trade and technology secrets to bolster their fortunes at U.S. expense.

The report’s unclassified version did not accuse Russia or China, nor blame any other country by name for allegedly targeting U.S. infrastructure like power grids, transportation hubs and telecommunications networks.

Alexander, who also heads the U.S. military’s Cyber Command, told the

Aspen Security Forum that he was unaware of any evidence that Stuxnet were now being turned against the United States, as some experts have predicted might be the case now that the malware has become available online.

Some of what the general called the 17-fold increase was attributed to nation states and some to "hackers and other criminals," he said.

"More right now (of attacks on infrastructure) is criminal and hackers ... the majority," Alexander said in reply to a question. "But not by a lot."

Alexander said earlier this month that the number of attacks on critical U.S. infrastructure went from nine in 2009 to more than 160 last year.

The general is headed to an annual conference in Las Vegas known as Defcon, a gathering of geeks, hackers and security professionals that amounts to the world's largest hacking party.

"We need them to help educate our country in cybersecurity," he said of the hackers' cyber savvy. "And I think there's some great things they can do."

Mac Malware Alert Surfaces as Mountain Lion Goes Live

Just as Mac OS X Mountain Lion is going live, security firm Sophos has identified a nasty piece of Mac malware.

The malware, known as Crisis and Morcut, arrived via a file named "AdobeFlashPlayer.jar." The "jar" in this case refers to "Java archive" and are just a ZIP file by another name, according to Sophos. In this case, opening the file will unleash a .class file named WebEnhancer, and "two unassuming-looking files named win and mac." The "mac" is an installer for Crisis or Morcut

However, the good news is that the WebEnhancer applet will trigger the digital signature alert below:

The researcher warns, though, that the malware doesn't necessarily have to be delivered via a ".jar" file -- that's just the way it came about in this case. If you do download Morcut/Crisis, then beware. According to Sophos, "Morcut has kernel driver components to help it hide, a backdoor component which opens up your Mac to others on your network, a command-and-control component so it can accept remote instructions and adapt its behaviour, data stealing code, and more."

Sophos warns Mac users not to assume that they're safe from malware attacks. Indeed, such threats have been on the rise as the platform has grown in popularity. Another piece of advice is to uninstall Java if you don't need it. "That leaves one less convenience for malware writers."

U.S. Spy Agency Chief To Meet with Hackers at "Defcon"

Computer geeks attending the world's largest annual hacking party in Las Vegas next week will have a rare chance to rub shoulders with the head of the U.S. National Security Agency.

General Keith Alexander, director of the spy agency, will speak at the Defcon conference, marking the highest-level visit to date by a U.S. government official to the colorful gathering. Organizers expect some 15,000 hackers this year as they celebrate the 20th anniversary of the first U.S. hacking event that was open to the public.

The Pentagon disclosed the visit on Friday.

"We’re going to show him the conference. He wants to wander around," said Jeff Moss, a hacker who organized the first Defcon conference while working as a messenger for a Seattle law firm. He now sits on an advisory committee to the Department of Homeland Security.

Alexander may choose to talk shop with the techies. He holds four master’s degrees, including ones in electronic warfare and physics.

Still, Moss said he expect there could be some controversy over Alexander’s presence among the diverse hacker crowd that attends the conference.

The NSA plays both offense and defense in the cyber wars. It conducts electronic eavesdropping on adversaries, in addition to protecting U.S. computer networks.

"I expect some people will say ’You are a sellout for having someone from the NSA speak," said Moss, who is known as the Dark Tangent in the hacking community.

But he doesn’t see it that way.

"One of the things I try to do at Defcon is take some of the hackers out of their comfort zone. I want to expose them to people they would normally not hear from," he said.

"Don’t you think it’s important to hear what the most senior person at the NSA has to say? I’m interested in hearing what he has to say," said Moss, whose full-time job is serving as chief security officer with ICANN, the Internet Corporation for Assigned Names and Numbers, which helps manage the infrastructure for much of the Internet.

Hackers come to the conference to exchange information about tools of the trade, socialize and compete in hacking contests.

There will be talks on attacking mobile phones and Google TV, more technical discussions on programming and discussions about government surveillance.

Defcon offers a side conference for children, Defcon Kids, which Alexander will likely visit. It also trains hackers to pick locks and has an annual contest to measure who is best at persuading corporate workers to release sensitive data over the phone.

Moss said he invited federal agents to the first Defcon conference, but that they politely declined. They showed up anyway, incognito. They kept coming, in bigger numbers, sometimes in uniform.

"We created an environment where the feds felt they could come and it wasn’t hostile," Moss said. "We could ask them questions and they wanted to ask the hackers about new techniques."

He said he’s spent a decade trying to get the head of the NSA to speak at Defcon, but he never imaged it would actually happen: "To me this is really validating of the whole culture."

Hackers Post Pilfered Yahoo! Passwords

Yahoo! on Thursday was digging into how hackers looted nearly a half million passwords and email addresses from one of its servers.

A hacker group calling itself D33DS posted online a massive trove of data it said was unencrypted in a file pilfered from the Sunnyvale, California-based Internet pioneer "as a wake-up call not as a threat."

Yahoo! confirmed that a file from its Contributor Network (formerly Associated Content) containing approximately 450,000 Yahoo! and other company users names and passwords was compromised on Wednesday.

Security researchers who sifted through the posted data determined that it included information about accounts at other online services including Google’s web-based Gmail, AOL, and Microsoft’s Live.com.

"We apologize to all affected users," Yahoo! said in a prepared statement.

"We are taking immediate action by fixing the vulnerability that led to the disclosure of this data, changing the passwords of the affected Yahoo! users and notifying the companies whose users accounts may have been compromised."

Less than five percent of the Yahoo! account data stolen had valid passwords, the company contended.

Affected accounts were reportedly at an Internet telephone service called Yahoo! Voices, which is related to the company’s instant messaging feature.

"The most alarming part to the entire story was the fact that the passwords were stored completely unencrypted and the full 400,000-plus usernames and passwords are now public," Internet security firm TrustedSec said in a blog post.

The hack came a month after a disturbing rash of security breaches in which members’ passwords were stolen from career-oriented social network LinkedIn as well as US dating website eHarmony and British-based music site Lastfm.com.

Security experts said in June that some 6.5 million LinkedIn accounts were posted to a Russian hacker forum.

Such data thefts are a bane to modern lifestyles that increasingly involve storing information and accessing services in the Internet "cloud."

Users of online accounts are urged by security experts and technology firms to select tough passwords and change them frequently to thwart hackers.

Athletes Urged To Think Twice Before They Tweet

Athletes racing to share their views with fans at the London Olympics may think twice before hitting send following the first expulsion of an athlete for a racist Twitter remark.

Greek triple jumper Paraskevi Papachristou was withdrawn from the London Olympics on Wednesday after causing an uproar in her home nation for a tweet about West Nile mosquitoes and the number of Africans in Greece.

Her expulsion was expected to act as a warning to other athletes who, along with Olympic organizers, are trying to find the best way to harness the power of social media that has exploded since the 2008 Beijing Games.

"The fact that this has happened will make other athletes feel more cautious about what they put out there," said Rebecca Hopkins, managing director of sports PR agency ENS Ltd that handles crisis media management.

"It is always very difficult to impose a limit on freedom of speech but the IOC (International Olympic Committee) has set down the guidelines and the athletes have to comply."

The explosion of social media in the past four years has created a new challenge for the IOC and for the National Olympic Committees who could previously resolve any indiscretions away from the public eye.

Since the Beijing Olympics, the number of Facebook users has surged to 900 million from 100 million and Twitter has 140 million users having only just emerged in 2008.

Aware that athletes and their fans are prolific users of social media, the IOC said competitors at the London Games may post, blog and tweet - but within guidelines.

Competitors may write "first-person, diary-type" entries but should not act as reporters, and social media activity must respect the Olympic Charter which condemns any discrimination. Vulgar or obscene words or images were also ruled out.

Postings deemed to be for commercial or advertising purposes were also on the no-go list.

The IOC made it clear that the accreditations of "any organization or person ... may be withdrawn without notice" if its guidelines are breached and most athletes were aware of the rules.

"The thing is you have to be careful with the social media side of things - certainly the decision to tweet or not tweet, and certainly what you say," said British badminton player, Imogen Bankier.

The sports world has seen a fair number of social media abuses in recent years particularly among soccer players.

The English Football Association and New Zealand rugby board responded by banning their players from using social media during recent football and rugby union World Cups.

So far only a handful of Olympians have landed in hot water.

Australian swimmer Stephanie Rice lost a lucrative endorsement deal with Jaguar two years ago after tweeting a comment seen as homophobic.

Australian swimmers Nick D'Arcy and Kenrick Monk have been banned from using social media in London by the Australian Olympic Committee after posting a photo of themselves brandishing guns on Facebook while training in the United States.

They have also been ordered to return home immediately after the completion of their events at London.

Athletes said Wednesday's expulsion would be a wake-up call but would not stop athletes form using social media at the Olympics.

"Most of us I think are pretty good about it, and I've seen a lot of people in the sports community use it pretty wisely," said Chas Betts, a U.S. Greco-Roman wrestler.

"I think it can be very beneficial, you know, updates and things ... so for the most part I think it's a good thing."

British Man Wins 'Twitter Threat' Appeal

A British man on Friday won a High Court challenge of his conviction for tweeting that he would blow up an airport if his flight was canceled, a ruling that had made him an Internet free speech cause celebre.

Paul Chambers, 28, was convicted and fined 385 pounds ($605) in 2010 over the tweet that he would blow up Robin Hood Airport in northern England, which he insisted was a joke. Thousands of Twitter supporters retweeted Chambers' message after he was convicted with the tag "I Am Spartacus" a reference to the 1960 movie epic in which the titular hero's fellow rebels all assume his identity in a gesture of solidarity.

His lawyer had argued before the High Court that if his tweet was considered menacing, then William Shakespeare could have been convicted for quipping, "Let's kill all the lawyers," in his play, "Henry VI."

High Court judges on Friday overturned Chambers' conviction, saying there was no evidence to suggest that anyone who saw the tweet found it to be menacing or alarming.

"I am relieved, vindicated it is ridiculous it ever got this far," Chambers said after the verdict.

U.K. celebrities such as broadcaster Stephen Fry and comedian Al Murray had also voiced their support for Chambers.

OS X Mountain Lion Makes Your Mac More Like Your iPhone Than Ever Before

As mobile devices like smartphones and tablets gradually add more and more features, and desktop and laptop operating systems continue to their attempt to simplify things, the two will inevitably cross paths. Mountain

Lion the latest updated to Mac OS X, available now through the Mac App Store brings us as close to that nexus point as we have ever been, but whether that's a blessing or a burden is largely up to you. These are the five new Mountain Lion features that are turning your Mac into a giant, even more expensive iPhone.

When the iPhone received the iOS 5 update, it killed popup notifications once and for all. Now, all the happenings on your phone including text messages, emails, and social network updates appear in a slick pull-down menu. With Mountain Lion, your Mac gets the same treatment.

You can customize your notification center to show updates for various applications including Facetime and Game Center, as well as calendar reminders and new email messages. You can even choose to post to social networks like Twitter or Facebook right from the notification window. The new feature is certainly convenient, but it also somewhat negates the need to browse the web in the same way you used to now that your Mac is so mobile-minded.

The Siri virtual assistant on the iPhone 4S is extremely helpful for finding information and composing short messages without having to physically interact with your smartphone, and while the full Siri experience isn't included in Mountain Lion, the voice dictation feature is making the leap to your Mac.

Using Dictation allows you to write notes, compose emails, and reply to chat conversations simply by speaking whatever it is you want to type. The benefits of using such an option on a mobile device are quite obvious you can probably speak faster than you can press the tiny virtual keys anyway but we can't help but wonder how many people will actually use it on their Macs, where your full keyboard is laying right in front of you.

In the same way that iOS 5 made everything on the iPhone instantly shareable via Facebook and Twitter, Mountain Lion allows you to push practically anything on your screen to your social network of choice. Find a web page your Twitter friends would enjoy, or a photo that you want to plaster on your Facebook profile? There's built-in buttons to do just that.

You can effectively update your social accounts without ever actually visiting your own profile page, which may cause a bit of a disconnect for users who frequently post, but rarely check replies. Built-in Twitter functionality is ready to go right now, while Facebook fanatics will have to wait a couple months before their favorite social network is added to Mountain Lion.

The introduction of iCloud was big news for iPhone users who wanted to sync things like reminders, and documents over multiple devices. With Mountain Lion, that same effortless syncing comes to Mac. With iCloud, your information remains constant over all your devices, meaning you can do things like update your iPhone's calendar, notes, and contacts right from your desktop or MacBook.

In the texting age, mobile messaging is a feature used daily by millions of people, and with the introduction of iMessage for Mac, Mountain Lion lets you chat with your iPhone-equipped compadres without ever touching your mobile device.

Once you sign in to iMessage on your Mac, you can send chat messages to anyone equipped with an iPhone or iPad. And rather than pecking away at

tiny touchscreen keys, you can rest your fingers on your Mac keyboard instead. Of course, while the ability to text from your laptop or desktop is convenient, the feature only lets you communicate with others who are using iMessage-compatible devices, which as of now are limited to the iPhone, iPad, and iPod Touch running iOS 5.

So what does the future hold, now that mobile and computer-based operating systems seem destined to collide? It’s hard to say. If Apple’s current trend of introducing new features on iOS before moving them to OS X continues, we need only to look to iOS 6 to know what the next version of Mac software will have to offer.

Facebook s Stock Is Tanking Did Investors Get Played by Big Banks?

Although Facebook (FB) met expectations in its first-ever earnings report on Thursday, the reaction from investors has been decidedly ugly so far. By the end of trading on Friday, the company s stock price had dropped by 117% to close at $23.70, or about half the value of its 52-week peak of $45. Making things worse, Facebook s big slide came on a day when the NASDAQ closed up 2.24%, meaning Facebook can t plausibly blame its slide on weak U.S. GDP numbers or other external factors.

As Forbes s Nathan Vardi notes, Facebook was never really in an ideal situation to go public this year and investment banks used the company s brand-name status to hype it to unreasonable expectations, especially given that no one knew whether the social networking giant had really figured out how to create a sustainable business model at the time.

And when investors learned yesterday that Facebook wouldn t be providing any third-quarter guidance despite the fact that its capital expenditures had ballooned by 213% year-over-year, well, that just had sell off written all over it.

The bottom line, then, is that investors aren t yet convinced that Facebook knows how to make sure its large investments will pay off in terms of revenue growth. And until that happens, early Facebook shareholders will likely continue to take a bath on their investments.

3 Million Lost Souls Still Trapped in AOL Dial-up Hell

Thankfully, most Internet users haven t been forced to hear the words Wel-come! You ve got mail! when they log onto the Web for at least a decade now. But Dan Fromer at SplatF has combed through AOL s (AOL) second-quarter earnings report and found that AOL still provides dial-up service to roughly 3 million subscribers. Granted, that number is a big drop from AOL s halcyon days when it counted more than 25 million subscribers and was sending around soon-to-be-coasterized AOL installation CDs with reckless abandon. But even so, who exactly is still stuck on AOL dial up these days, and can we organize a satellite service rescue charity to help these poor suckers out?

Who Really Invented the Internet?

Contrary to legend, it wasn’t the federal government, and the Internet had nothing to do with maintaining communications during a war.

A telling moment in the presidential race came recently when Barack Obama said: "If you’ve got a business, you didn’t build that. Somebody else made that happen." He justified elevating bureaucrats over entrepreneurs by referring to bridges and roads, adding: "The Internet didn’t get invented on its own. Government research created the Internet so that all companies could make money off the Internet."

It’s an urban legend that the government launched the Internet. The myth is that the Pentagon created the Internet to keep its communications lines up even in a nuclear strike. The truth is a more interesting story about how innovation happens and about how hard it is to build successful technology companies even once the government gets out of the way.

For many technologists, the idea of the Internet traces to Vannevar Bush, the presidential science adviser during World War II who oversaw the development of radar and the Manhattan Project. In a 1946 article in The Atlantic titled "As We May Think," Bush defined an ambitious peacetime goal for technologists: Build what he called a "memex" through which "wholly new forms of encyclopedias will appear, ready made with a mesh of associative trails running through them, ready to be dropped into the memex and there amplified."

That fired imaginations, and by the 1960s technologists were trying to connect separate physical communications networks into one global network a "world-wide web." The federal government was involved, modestly, via the Pentagon’s Advanced Research Projects Agency Network. Its goal was not maintaining communications during a nuclear attack, and it didn’t build the Internet. Robert Taylor, who ran the ARPA program in the 1960s, sent an email to fellow technologists in 2004 setting the record straight: "The creation of the Arpanet was not motivated by considerations of war. The Arpanet was not an Internet. An Internet is a connection between two or more computer networks."

If the government didn’t invent the Internet, who did? Vinton Cerf developed the TCP/IP protocol, the Internet’s backbone, and Tim Berners-Lee gets credit for hyperlinks.

But full credit goes to the company where Mr. Taylor worked after leaving ARPA: Xerox. It was at the Xerox PARC labs in Silicon Valley in the 1970s that the Ethernet was developed to link different computer networks. Researchers there also developed the first personal computer (the Xerox Alto) and the graphical user interface that still drives computer usage today.

According to a book about Xerox PARC, "Dealers of Lightning" (by Michael Hiltzik), its top researchers realized they couldn’t wait for the government to connect different networks, so would have to do it themselves. "We have a more immediate problem than they do," Robert Metcalfe told his colleague John Shoch in 1973. "We have more networks than they do." Mr. Shoch later recalled that ARPA staffers "were working under government funding and university contracts. They had contract administrators . . . and all that slow, lugubrious behavior to contend with."

So having created the Internet, why didn’t Xerox become the biggest

company in the world? The answer explains the disconnect between a government-led view of business and how innovation actually happens.

Executives at Xerox headquarters in Rochester, N.Y., were focused on selling copiers. From their standpoint, the Ethernet was important only so that people in an office could link computers to share a copier. Then, in 1979, Steve Jobs negotiated an agreement whereby Xerox's venture-capital division invested $1 million in Apple, with the requirement that Jobs get a full briefing on all the Xerox PARC innovations. "They just had no idea what they had," Jobs later said, after launching hugely profitable Apple computers using concepts developed by Xerox.

Xerox's copier business was lucrative for decades, but the company eventually had years of losses during the digital revolution. Xerox managers can console themselves that it's rare for a company to make the transition from one technology era to another.

As for the government's role, the Internet was fully privatized in 1995, when a remaining piece of the network run by the National Science Foundation was closed just as the commercial Web began to boom. Blogger Brian Carnell wrote in 1999: "The Internet, in fact, reaffirms the basic free market critique of large government. Here for 30 years the government had an immensely useful protocol for transferring information, TCP/IP, but it languished. . . . In less than a decade, private concerns have taken that protocol and created one of the most important technological revolutions of the millennia."

It's important to understand the history of the Internet because it's too often wrongly cited to justify big government. It's also important to recognize that building great technology businesses requires both innovation and the skills to bring innovations to market. As the contrast between Xerox and Apple shows, few business leaders succeed in this challenge. Those who do not the government deserve the credit for making it happen.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.